(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10126406 A**

(43) Date of publication of application: **15 . 05 . 98**

(51) Int. Cl **H04L 9/14**
H04L 9/08

(21) Application number: **08299505**

(22) Date of filing: **23 . 10 . 96**

(71) Applicant: **TOYO COMMUN EQUIP CO LTD**

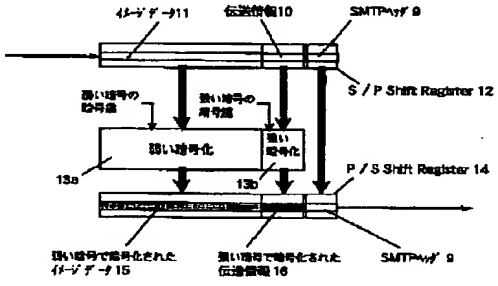
(72) Inventor: **MORIZUMI TETSUYA**
YASUI TSUGUNORI

(54) **DATA CIPHER SYSTEM IN NETWORK**

(57) Abstract:

PROBLEM TO BE SOLVED: To limit time that is needed for encipher and decoding at a transmission destination without damaging the confidentiality of data through encipher by making data image data and inserting the key of cryptograph of the data into transmission information.

SOLUTION: This system is provided with a serial in parallel out shift (S/P) register 12, encipher processing parts 13a and 13b and a parallel in serial out (P/S) register 14. It does not perform any encipher to an SMTP header 9 which does not need security, performs strong encipher to transmission information 10 which includes much significant information in the part 13b, performs weak encipher to image data 11 in the part 13a and then moves the contents from the S/P register 12 to the P/S register 14. That is, it performs a strong cipher system such as elliptic cipher, an RSA, a DES and nonlinear shift register to the transmission information 10 and performs a weak cipher system such as a linear shift register, simple inversion and replacement to the image data 11.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－126406

(43)公開日　平成10年(1998)５月15日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00		６４１
9/08				６０１Ｃ

審査請求　未請求　請求項の数３　ＦＤ　（全　４　頁）

(21)出願番号　特願平8－299505

(22)出願日　平成８年(1996)10月23日

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号

(72)発明者　森住　哲也
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内

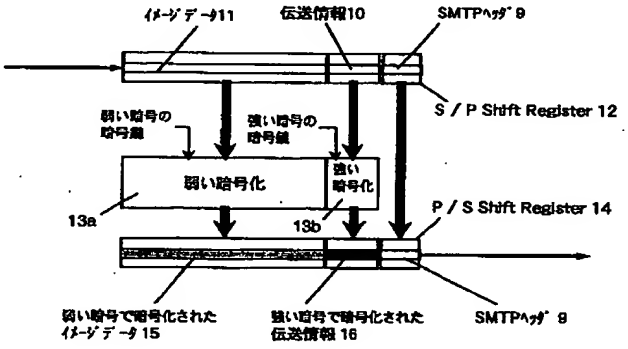
(72)発明者　安井　嗣了
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内

(54)【発明の名称】　ネットワークにおけるデータの暗号方式

(57)【要約】

【目的】イメージデータのような膨大なデータ量を呈する情報を伝送する場合であっても、暗号化によるデータの秘匿性を損なうことなく暗号化及び伝送先での復号化に要する時間を極限する暗号方式を提供することを目的とする。

【構成】伝送すべきデータに伝送情報を付与し、これをネットワーク上に接続した端末間で送受信するシステムに於いて、前記伝送情報に施す暗号の強さを前記データに施すそれよりも強くしたネットワークにおけるデータの暗号方式であって、特に、前記データがイメージデータであること、若しくは前記伝送情報に前記データの暗号鍵を挿入したものである。



1

【特許請求の範囲】

【請求項１】伝送すべきデータに伝送情報を付与し、これをネットワーク上に接続した端末間で送受信するシステムに於いて、前記伝送情報に施す暗号の強さを前記データに施すそれよりも強くしたことを特徴とするネットワークにおけるデータの暗号方式。

【請求項２】前記データがイメージデータであることを特徴とする請求項1記載のネットワークにおけるデータの暗号方式

【請求項３】前記伝送情報に前記データの暗号鍵を挿入したことを特徴とする請求項1又は2記載のネットワークにおけるデータの暗号方式

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークにおけるデータの伝送、特にイメージデータの暗号化方式に関する。

【０００２】

【従来の技術】近年、インターネット等、広域ネットワーク整備され、これを利用したデータの伝送が一般的に行われるようになった。図４はインターネットを利用した端末間のファクシミリ情報の伝送システムの形態を示す概念図である。

【０００３】端末1は、予め用意したデータ(テキスト、イメージ)をインターネット2を介して他の端末3あるいはゲートウェイ4を経由してFAX装置5に伝送する。

【０００４】端末1は図５に示すようなフレームフォーマットのデータを用意する。伝送すべきイメージデータ6の直前に伝送先或いは送信元の情報(FAX番号、パスワード、ユーザ名等)を記載した伝送情報7を付与し、更にその直前にインターネットのメールのプロトコル(RFC0821)で規定されたSMTPヘッダ8を付与しておく。

【０００５】周知の通り、インターネットはオープンなネットワーク環境であり、メールは不特定の複数のサーバを経由して伝送先まで送達されることになるので、クローズドな熱とワークに比して秘匿性が著しく低いという欠点がある。そこで、インターネットを商用などに利用する場合は、何らかのセキュリティ(暗号化)が必要となる。従来、一般的にはSMTPヘッダより後の伝送情報とイメージデータに対して所定の暗号化を施した上で伝送していた。

【本発明が解決しようとする課題】

【０００６】しかしながら、上述したようにイメージデータのような膨大なデータ量を呈する情報を伝送する場合には、暗号化及び伝送先での復号化に時間がかかるという欠点があった。このため、ユーザーが長時間データの到着を待たされる、あるいは、通信処理に加えて暗号化及び復号化処理が必要であるために、通信装置自体に大きな負担がかかるといった問題が生じていた。この問題に対処すべく、例えば比較的弱い暗号化方式を用いれば、上述の処理時間を短縮することが可能であるが、伝送情報7にはプライバシーに関わる情報やクレジットカード番号などの極めて重要な情報が含まれる場合が多い。従って、この例の様な弱い暗号化方式では安全性が不十分である為、依然として強い暗号方式を用いなければならず、上述の問題点を解決するには至っていないのである。本発明はイメージデータのような膨大なデータ量を呈する情報を伝送する場合であっても、暗号化によるデータの秘匿性を損なうことなく暗号化及び伝送先での復号化に要する時間を極限する暗号方式を提供することを目的とする。

2

【０００７】

【課題を解決するための手段】伝送すべきデータに伝送情報を付与し、これをネットワーク上に接続した端末間で送受信するシステムに於いて、前記伝送情報に施す暗号の強さを前記データに施すそれよりも強くしたネットワークにおけるデータの暗号方式であって、特に、前記データがイメージデータであること、若しくは前記伝送情報に前記データの暗号鍵を挿入したことを特徴とするものである。

【０００８】

【発明の実施の形態】図１は本発明にかかる暗号化方式の暗号化処理装置の一実施例の概念を示す図面である。同図において12はシリアルイン・パラレルアウトシフトレジスタ（S/Pレジスタ）であって、図中左方のデータ生成部（図示しない）より到来したSMTPヘッダ9と伝送情報10とイメージデータ11が保持されている状態を示している。13a、13bは暗号化処理部であって、13aは弱い暗号化を、13bは強い暗号化をそれぞれ施すものである。14はパラレルイン・シリアルアウトシフトレジスタ（P/Sレジスタ）であって、暗号化処理部13a、13bにて暗号化を施したデータを保持しデータ列として次段に送出するものである。　この暗号化装置は以下のように動作する。セキュリティの必要のないSMTPヘッダ9については暗号化を施すことなくそのまま、重要な情報を多く含む伝送情報10については暗号化処理部13bにて強い暗号化を施した上で、イメージデータ11については暗号化処理部13aにて弱い暗号化を施した上でS/Pレジスタ12からP/Sレジスタ14へ内容を移動する。具体的には、楕円暗号、RSA, DES、非線形ｼﾌﾄﾚｼﾞｽﾀといった強い暗号方式を伝送情報10に、線形ｼﾌﾄﾚｼﾞｽﾀ、簡単な転置、換置といった弱い暗号方式をイメージデータ11に施せばよい。このような暗号方式を施すことによって伝送情報10については強い秘匿性を維持しつつ、データ量が比較的の少ないので暗号化に要する処理時間はわずかであり、イメージデータ11についても弱い暗号化を施すのみであるから処理時間を大幅に短縮することが可能である。

【０００９】図２は本発明にかかる暗号化方式の復号化処理装置の概念を示す図面であり、S/Pレジスタ21とP/Sレジスタ24の間に、弱い暗号化を復号する復号化処理部

22aと、強い暗号化を復号する復号化処理部22bとを配置し、暗号化が施されたデータを元のデータ形式に復号するものである。この装置を用いることによって伝送先における復号化も上述の暗号化と同様にその処理時間を大幅に短縮することが可能となることは自明である。

【００１０】また、図３（a）、（b）に示すように、伝送情報10にイメージデータに施す弱い暗号化方式の復号鍵を記述しておくことで、弱い暗号方式の秘匿性を高めることもできる。例えば、弱い暗号化であってもその暗号鍵すなわちこれを解読する為の復号鍵をランダムに頻繁に変更することで暗号としての秘匿性を高めることができるのである。

【００１１】更に、このとき伝送情報10の強い暗号化の暗号鍵はSMTPヘッダ9に記述して伝送することもできる。尚、以上本発明をイメージデータをインターネットを介して伝送する場合を例に説明したが、本発明はこれのみに限定されるものではなく、動画や音声と云った他の如何なるデータであってのもよく、インターネット以外のネットワークに適用可能なこと説明するまでもない。また、SMTPヘッダには一切暗号化を施さない例を示したが、適宜暗号化を施しても良い。

【００１２】

【発明の効果】以上、本発明は上述したように構成するものであるから、イメージデータのような膨大なデータ量を呈する情報を伝送する場合であっても、暗号化によ＊るデータの秘匿性を損なうことなく暗号化及び伝送先での復号化に要する時間を極限する上で著しい効果を奏する。また、ユーザーが長時間データの到着を待たされるといった不具合が解消でき、通信装置自体にかかる負担を大幅に低減することもできる。

【００１３】

【図面の簡単な説明】

【図１】本発明にかかる暗号化方式の暗号化処理装置の一実施例の概念を示す図面。

【図２】本発明にかかる暗号化方式の復号化処理装置の一実施例の概念を示す図面。

【図３】（ａ）、（ｂ）は本発明にかかる暗号化方式の他の実施例の概念を示す図面。

【図４】インターネットを利用した端末間のファクシミリ情報の伝送システムの形態を示す概念図。

【図５】データのフレームフォーマットの例を示す図。

【符号の説明】

６、１１　・・・　イメージデータ

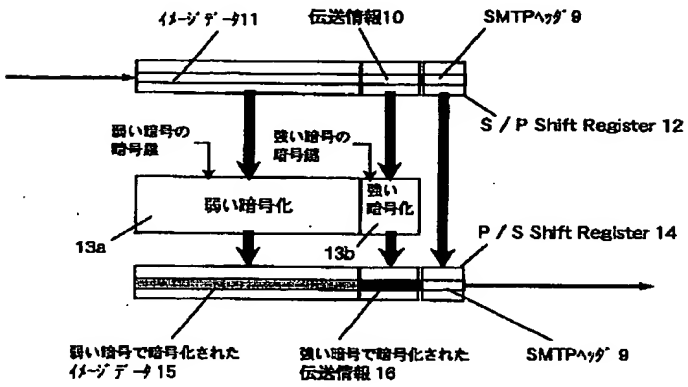
７、１０　・・・　伝送情報

８、９　・・・　SMTPヘッダ

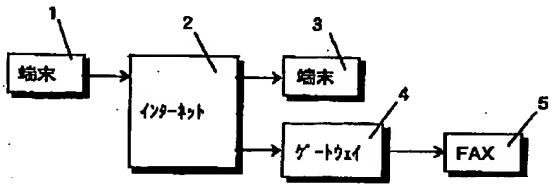
１２、２１、３１、４１・・・シリアルイン・パラレルアウトシフトレジスタ（S/Pレジスタ）

１４、２３、３４、４４・・・パラレルイン・シリアルアウトシフトレジスタ（P/Sレジスタ）

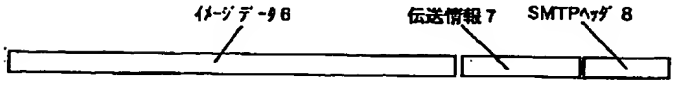
【図１】



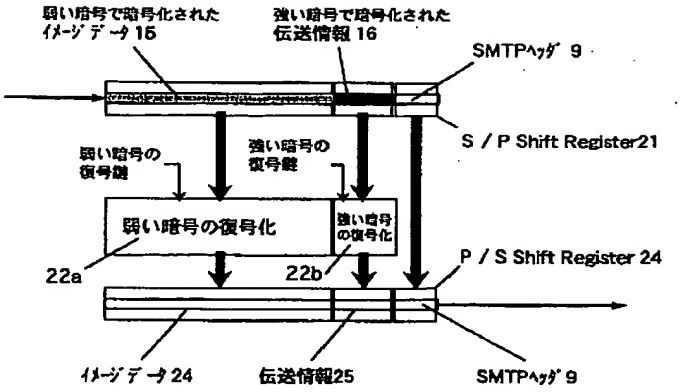
【図４】



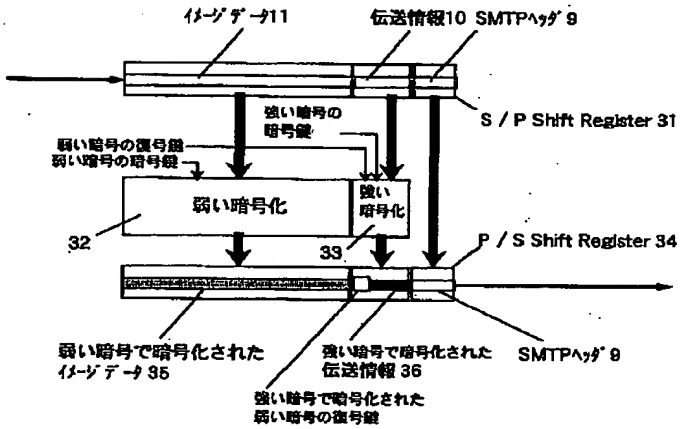
【図５】



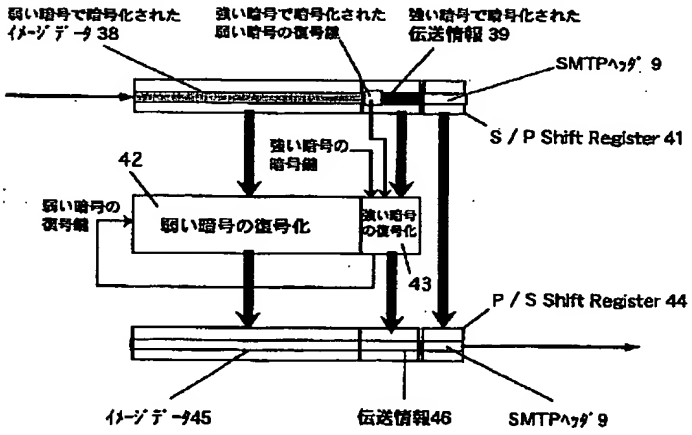
【図２】


弱い暗号で暗号化された
ｲﾒｰｼﾞﾃﾞｰﾀ 15
強い暗号で暗号化された
伝送情報 16
SMTPﾍｯﾀﾞ 9
S / P Shift Register21
弱い暗号の
復号鍵
強い暗号の
復号鍵
弱い暗号の復号化
強い暗号
の復号化
22a
22b
P / S Shift Register 24
ｲﾒｰｼﾞﾃﾞｰﾀ 24
伝送情報25
SMTPﾍｯﾀﾞ 9

【図３】


ｲﾒｰｼﾞﾃﾞｰﾀ11
伝送情報10
SMTPﾍｯﾀﾞ 9
S / P Shift Register 31
強い暗号の
暗号鍵
弱い暗号の復号鍵
弱い暗号の暗号鍵
弱い暗号化
強い
暗号化
32
33
P / S Shift Register 34
弱い暗号で暗号化された
ｲﾒｰｼﾞﾃﾞｰﾀ 35
強い暗号で暗号化された
伝送情報 36
SMTPﾍｯﾀﾞ 9
強い暗号で暗号化された
弱い暗号の復号鍵

(a)


弱い暗号で暗号化された
ｲﾒｰｼﾞﾃﾞｰﾀ 38
強い暗号で暗号化された
弱い暗号の復号鍵
強い暗号で暗号化された
伝送情報 39
SMTPﾍｯﾀﾞ 9
S / P Shift Register 41
42
強い暗号の
暗号鍵
弱い暗号の
復号鍵
弱い暗号の復号化
強い暗号
の復号化
43
P / S Shift Register 44
ｲﾒｰｼﾞﾃﾞｰﾀ45
伝送情報46
SMTPﾍｯﾀﾞ 9

(b)